RUTGERS
UNIVERSITY | NEW BRUNSWICK

Eagleton Institute OF Politics

Building the Resilience of Citizens, Communities, and Countries
A Rutgers Longitudinal Study of Principle-Based Policies and Practices
Chapter One: Houses of Worship and Vulnerable Communities

ACTION GUIDE

Dr. Ronald J. Clark

Terrorism and mass violence cannot prevail if people refuse to be terrorized. If people are resilient, if they return to their houses of worship, the assailant fails...

- Jeh Johnson, Former Secretary of the U.S. Department of Homeland Security

TABLE OF CONTENTS

Building the Resilience of Citizens, Communities, and Countries

A Rutgers Longitudinal Study of Principle-Based Policies and Practices

Action Guide for Houses of Worship Serving Vulnerable Communities

INTRODUCTION: RESILIENCE MODEL

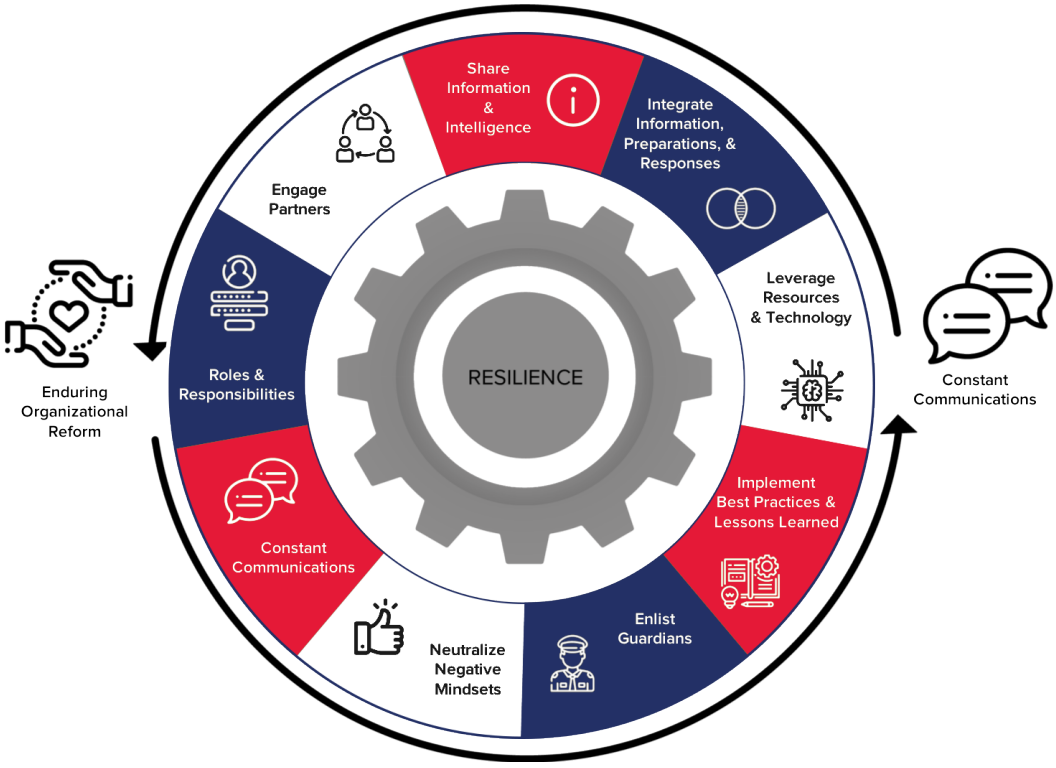
The research findings and attack statistics indicate a significant rise in threats to houses of worship and vulnerable communities. While longer lead policy efforts at the national level attempt to curb this rise in violence, houses of worship need to take prudent measures to ensure the security and safety of their respective communities. The RESILIENCE Model offers an evidence-based system that can, with minimal resources, enhance the security of houses of worship and vulnerable communities. Its ten principles, grounded in evidence and experience, offer a series of lighthouses that can move a community toward safer waters. The principles serve as guideposts and the corresponding material a path for execution. Further, this report can serve as a standalone guide or it can integrate and be complemented by a broad range of well-produced security reports, manuals, and checklists.

The RESILIENCE Model can be put into action through a linear execution from the first to the tenth principle. Here the journey starts with the first principle, which focuses on roles and responsibilities, then partners, and on through the next seven principles. Admittedly, the sequencing of the principles is intended to have a logical order where one builds upon the next. Arguably, the RESILIENCE Model is most impactful when the system is executed in this order. However, putting the RESILIENCE Model into action need not be a lockstep process. The principles can be executed in alternate sequences based on priorities, gaps in existing security efforts, and the availability of internal or external resources. Whether the plan of action is linear or prioritized based on unique challenges and opportunities, the key is to take action. Start putting the evidence-based principles of the RESILIENCE Model to work today. Cumulatively, the RESILIENCE Model principles enable a strategic path to a resilient community.

The RESILIENCE Model Principles

To enable rapid communications and facilitate retention, the author developed the principles of the Clark Resilience Model. Once the principles were in position, he next crafted them into an acronym and model. The acronym became R.E.S.I.L.I.E.N.C.E. as the intent was to make it easy to communicate, remember, and act upon. The model became an interconnected set of principles or gears set in a circle. cities. From this initial chapter, the study will build across domains and sectors, culminating in evidence-based principles and practices for national resilience in future reports.

1. Roles and Responsibilities
2. Engage Partners
3. Share Information and Intelligence
4. Integrate Information, Preparations, and Responses
5. Leverage Resources and Technology
6. Implement Best Practices and Lessons Learned
7. Enlist Guardians and Execute the Plan
8. Neutralize Negative Mindsets
9. Constant Communications
10. Enduring Organizational Reform



PRINCIPLE ONE: ROLES AND RESPONSIBILITIES

The first principle of the RESILIENCE Model is "Roles and Responsibilities." To ensure the resilience of houses of worship, the identification of key security roles and the assigning of responsibilities is essential. The first step is to get organized and align the right people with the right roles and responsibilities. Think of it as "who is doing what, to who, when, and under what conditions."

Internal and External Stakeholders

Heads of congregations or religious leaders have a broad family of internal and external stakeholders that should be mapped and engaged. This natural team of stakeholders provides a range of options from organizing an institution's security to communications roles.

Organization of Roles

There are seven key roles, with associated responsibilities, that can be supported by an individual director for each one or consolidated into just two people. If the seven roles and responsibilities are consolidated into two people, one would serve as the Chief Security Officer and the other as the Chief Communications Officer.

Two Key Officers

- ✔ **Chief Security Officer (CSO)**
  - Roles: Security, Cyber Security, Information, and Plans
- ✔ **Chief Communications Officer (CCO)**
  - Roles: Communications, Resource Management, and Administration

The Board of Seven (Alternative Structure):

- ✔ **Director of Security**
  - Responsible for all aspects of safety and physical security preparations and responses.
- ✔ **Director of Cyber Security**
  - Responsible for all aspects of cyber security preparations and responses.
- ✔ **Director of Communications**
  - Responsible for all communications in steady state and in crisis.
- ✔ **Director of Information**
  - Responsible for the sharing, receiving, processing, and integrating of all information.
- ✔ **Director of Plans, Policies, and Training**
  - Responsible for all assessments, plans, training, and exercises.
- ✔ **Director of Resource Management**
  - Responsible for all security and safety-related resource management from external grants to internal funding.
- ✔ **Director of Administration**
  - Responsible for all aspects of safety and security administration.

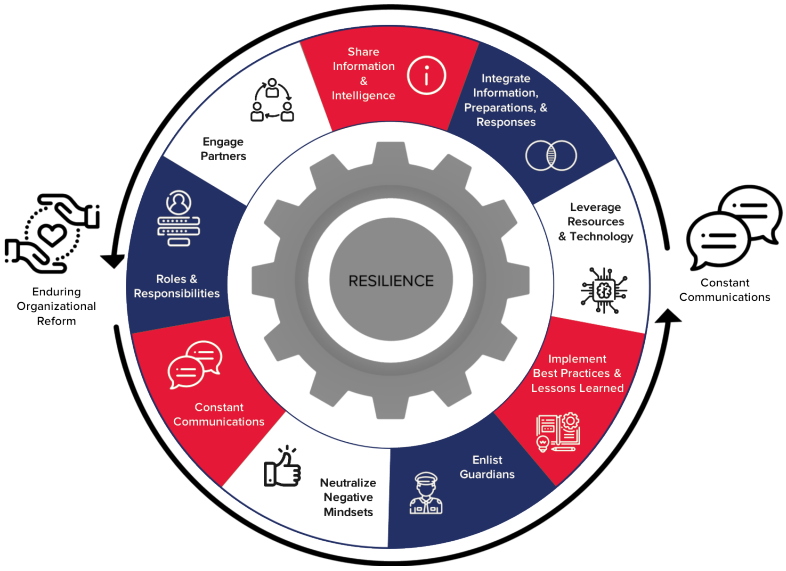
Establish Key Teams: Every role and its corresponding director or chief are supported by a team. The teams consist of internal and external stakeholders.

Establish Key Committees: Any number of committee structures are viable for a house of worship (e.g. security and planning). Some committees will be permanent, while others are constituted as needed (e.g. assessment and crisis).

Take Action!

- ✔ Institution: Assign Roles and Responsibilities.
- ✔ Institution: Identify "Who's in Charge? Of What? When?
- ✔ Institution: Build a Team for the Chiefs and Directors
- ✔ Institution: Establish Committees for Assessment & Crisis
- ✔ Institution: Coordinate Roles and Responsibilities with External Stakeholders.
- ✔ Individual: Know One's Roles and Responsibilities.
- ✔ Individual: Know Who is Responsible for What, When.

> *Someone at the house of worship or charity should be aware of the risks they are facing. Someone should have that charge.*
>
> *- Andy Jabbour, Cofounder, FB-ISAO*



PRINCIPLE 2: ENGAGE PARTNERS

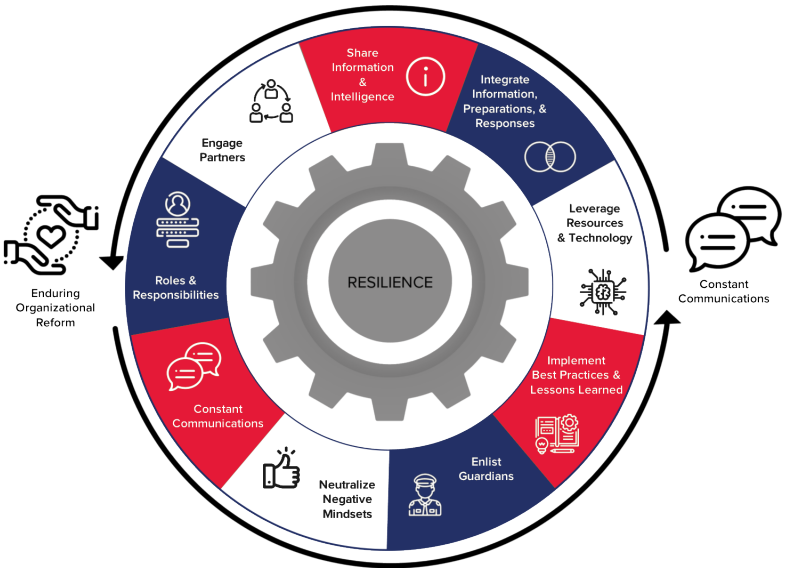
The second principle of the RESILIENCE Model is "Engage Partners." Its focus is on building partnerships and creating relationships, within the congregation and community. It is about engaging local partners, state stakeholders, and Federal organizations. The "Engage Partners" principle sits at the core of the RESILIENCE Model. It enables the implementation of the other nine principles. Houses of worship are fortunate to have a natural link to a broad range of partners who are willing to support and want to help. They just need to be engaged and invited into the community. Frequently, the enduring gap is a systemic failure to reach out, to connect, and to engage natural partners. Unify under the mantra that an attack on one house of worship is an attack on all!

- ✔ **Step One Identify, Index, and Optimize Existing Partnerships:** The first step is to identify, index, and optimize existing partnerships (congregation, community, first responders).
- ✔ **Step Two Expand Partnerships Internally:** The next step is to expand upon existing partnerships, both internally and externally.
- ✔ **Three Expand Partnerships Externally – Locally, Federally, and Internationally:** With existing partnerships optimized and internal ones expanded, the next piece is to engage external partners.

Take Action!

- ✔ Engage Partners.
- ✔ Identify, Index, and Optimize Existing Partnerships.
- ✔ Engage Internal Partners.
- ✔ Engage External Partners.
- ✔ Ensure Institutional Level Partnering
- ✔ Form or Join a Faith-Based Council
- ✔ **Build Relationships.**

> *Be a part of your communities. Step out. Teach your kids. We're all in this together and when we're all in this together, you have a resilient community.*
>
> *- Russ Deyo, Former Deputy Secretary, U.S. Department of Homeland Security*



PRINCIPLE 3: SHARE INFORMATION AND INTELLIGENCE

The third principle of the RESILIENCE Model is to "Share Information and Intelligence." Gathering and sharing information helps mitigate the threat, build connections, and buttress vulnerable communities and houses of worship in times of crisis. It builds awareness and mutual trust. The goal of the third principle is to build situational awareness that enables action!

Sharing Information Protocols

- ✔ Step 1: Internally, the Head of the Congregation, Director of Security, and Director of Communications need to create a two-way flow of information with the members of their community.
- ✔ Step 2: Members of the community need to be empowered to share information and trained on suspicious reporting.
- ✔ Step 3: Externally, houses of worship need to routinize communications with external partners.

> *We need to share and disseminate information about the threat. We need to emphasize the importance of cooperation between law enforcement, the public, and the community, especially potential targeted communities and faith-based leaders and organizations.*
>
> *- Ali Soufan, Former FBI Agent*

Three-Step Information Cycle – Gather, Analyze, Share (GAS)

The GAS information and intelligence cycle consists of three steps: Gather, Analyze, and Share. The GAS acronym is a streamlined version of a more complex, traditional, and multi-step intelligence cycle that is contextually bound, cumbersome for smaller institutions, and a poor fit for houses of worship.

- ✔ **Gather Information**. Information should come from multiple sources and partners.
- ✔ **Analyze the Information.** Make sense of the information for your team, partners, and congregation.

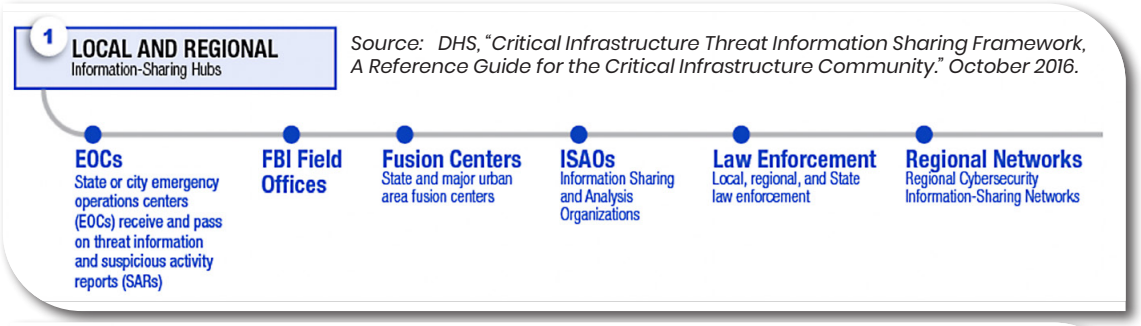
- ✔ **Share Information**. Distribute information internally and externally with partners, team members, and the broader community.

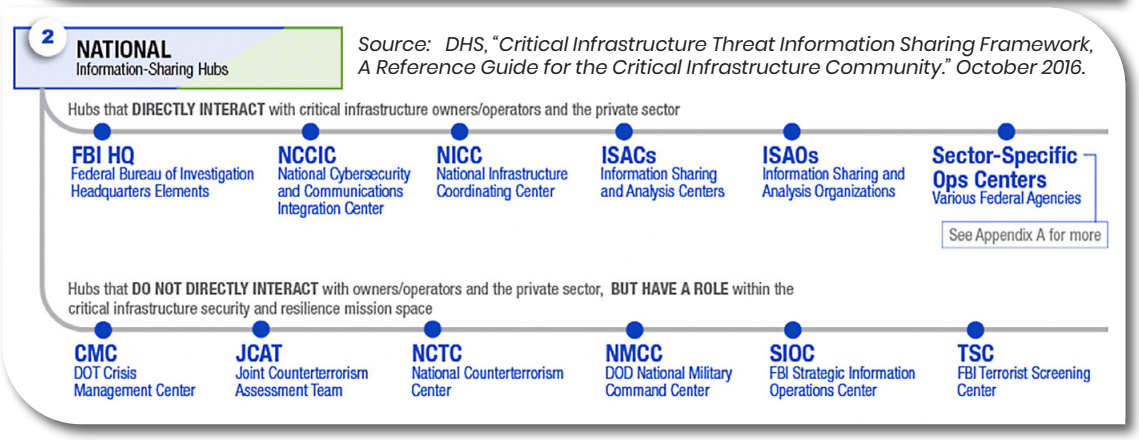
Reduce Complexity. The enactment of the principle need not be overly complex as it only requires a table, a place to meet and the right partners. A command center is not necessary.

UNNECESSARY

NECESSARY

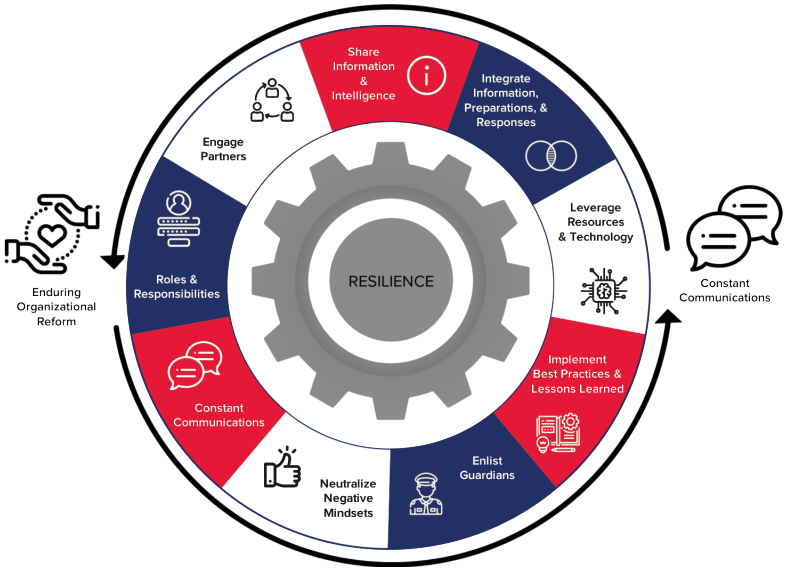
Examples of Information-Sharing Hubs





Take Action!

- ✔ Commit to the Sharing of Information.
- ✔ Establish Sharing Protocols
- ✔ Identify and Engage Local, Regional and National Information Sharing Hubs
- ✔ **Step on the GAS Acronym**
  - Gather Information.
  - Assess Information.
  - Share Information.
- ✔ Join FB-ISAO.



PRINCIPLE 4: INTEGRATE INFORMATION, PREPARATIONS, AND RESPONSES

The fourth principle of the RESILIENCE Model is "Integrate Information, Preparations, and Responses." The centrality of this principle is at the core of the RESILIENCE Model.

Information-Driven Preparations and Responses

With roles established, partners engaged and information sharing in place, it is time to create information-driven preparations and responses. Preparations include planning, training, and the exercising of responses. Resilience is dependent upon **awareness and action.**

> *There have to be crisis management plans, and they have to be coordinated, between authorities – across and between faith-based communities and the authorities.*
>
> *- Jonathan Fischer, Former House of Worship Head of Security (Copenhagen)*

Preparations — Key Concepts

- ✔ **You Must Assess to Achieve Success.** Assessment is the first critical preparation step. The assessment should address the ten principles of the RESILIENCE Model.
- ✔ **Think Like an Attacker:** Red Team All Plans and Assessments. Assess the veracity of your preparations and potential responses through the eyes of a potential attacker.
- ✔ **Identify and Disrupt the Reconnaissance Phase:** Adversary Signatures. This phase of an attack creates a distinct signature. When noted by aware personnel who act on these anomalous behaviors, it can lead to disruption directly or indirectly. Vigilance, presence, cameras, and simple door locks are powerful deterrents.

Preparations – Plans from Steady State to Crisis

> *Have a plan, rehearse your plan, and after you've rehearsed your plan, improve your plan.*
>
> *- Kona Zoganas, House of Worship Director of Security*

Establish Steady State Plans

- ✔ **Daily Operations.** The safety and security plans for daily operations form the foundation for all other plans.
- ✔ **Special Services and Events.** Special services and events are often routinized events and include a larger than average concentration of citizens and warrant enhanced security protocols.
- ✔ **Large Public Gathering**. Plans for large gatherings address the need for enhanced safety and security protocols during periods of unique concentration of a congregation or community.

Establish Crisis Response Plans

- ✔ **Crisis Response Plans.** These plans allow a house of worship to prepare for extremely disruptive, yet infrequent, events. House of worship crisis response plans include fire evacuation, active threat, improvised explosive devices, and natural disaster. Crisis response plans are distinct in their need for precision, the compression of time, and consequences.

Establish Contingency Plans

- ✔ **Succession Plan.** Succession plans ensure continuity and identifies a primary, alternate, and tertiary lead for security and communications.
- ✔ **Communications Plan.** Speaking with one voice before, during, and after crisis to address key basics that include: Who is communicating? What are they communicating? When? Why?

Establish Awareness Plans. Sense It! Identify Suspicious Behavior! Push Out Your Perimeter!

- ✔ Establish awareness plans to empower every person to be part of the safety and security.
- ✔ Build out a simple set of awareness protocols and reporting.
- ✔ Integrate technology.

Establish Natural Disaster Planning and Plans

- ✔ Just as Federal and state emergency management teams conduct annual assessments of community vulnerabilities, so too must vulnerable communities also understand the threats posed by natural hazards, public health emergencies such as pandemics, biological and chemical accidents, radiological and nuclear hazards, or severe weather events such as winter storms, hurricanes, earthquakes, tornadoes, floods, droughts, and wildfires.

Clark Rapid Planning Process – Clark Assess-Plan-Act (CAPA)

Why Do We Plan? We plan to prepare. We plan to align limited resources against prioritized threats, challenges, and opportunities.

How Do We Plan? The Clark Rapid Planning Process for communities provides a repeatable and simple three-step process.

- ✔ **Step 1: Assess**
  Assessments identify threats, challenges, resources, strengths, and weaknesses – sets up "the plan."
- ✔ **Step 2: Plan**
  Step two takes the assessment and builds ways to address security gaps and reinforce strengths. Three key parts: Build, Review, and Select the best option.
- ✔ **Step 3 Act:**
  The final step in the CAPA planning process is to "ACT!" A straightforward bulleted document or slides are fast and easy to develop for implementation.
  Integrated Plans and Planning: Individual plans must be integrated across the broader range of plans, include physical and cyber security and coordinated with all stake holders.

> *Planning is the art and science of envisioning a desired future and laying out effective ways of bringing it about.*
>
> *- Marine Corps Doctrinal Publication (MCDP-5) Planning*

Train and Exercise

Training – The Three "Its": Sense It, Map It, Lock It (SML)

- ✔ ***"Sense It"*: Awareness Training and Technology.**
  - Disseminate suspicious behavior training across the community.
  - Train the congregation, greeters, and ushers to identify anomalous behavior.
  - "Sense It" is enhanced through the deployment of technology like cameras.
  - Establish a Suspicious Activity Reporting (SAR) program.

- ✔ ***"Map It"*: Integrate, Coordinate, and Execute Plans.**
  - The internal team and the external team, which includes first responders, need a common physical structure map (grid or blueprint) to prepare and respond.

- ✔ ***"Lock It":*** The bottom line is that locked doors work, and it is a timeless security measure.

Action Focused Training. Learn to Protect Self, Others, Community.

Active Threat Training:

- ✔ A series of options within "Run, Hide, Fight" and/or "Deter, Deny, Defend."

Bomb or Improvised Explosive Devices (IED) Training:

- ✔ Establish IED awareness and reporting training.
- ✔ Rapidly and reliably report all threats.

> *I'm a big fan of run, hide, fight. I think it's good to learn, and you should have a well trained and experienced person teach it to the congregation.*
>
> *– Roger Parrino, Former NY State Head of Emergency Management*

Medical Training: Institute basic medical training. Consider advanced trauma care training.

Fire and Arson Training:

- ✔ Review and Update Fire evacuation plans, routes, and alarms.

Cyber Training:

- ✔ Gain awareness of the threat and their tactics.
- ✔ Provide practical mitigation measures.

Exercises: Exercise the plans, the training and most importantly, the people.

- ✔ **Meet and Talk.**
- ✔ **Tabletop Exercises.**
- ✔ **Limited-Scale Exercises.**
- ✔ **Full-Scale Exercises.**

> *There's zero awareness! People have no idea regarding their significant cyber risks. And worse, people just automatically assume, well, that only happens to big companies. That doesn't happen to us. You know, nobody would care about us. I hear that all the time. Clients have been breached? Well, nobody would care about us.*
>
> *– Brian Dykstra, CEO Atlantic Data Forensics*

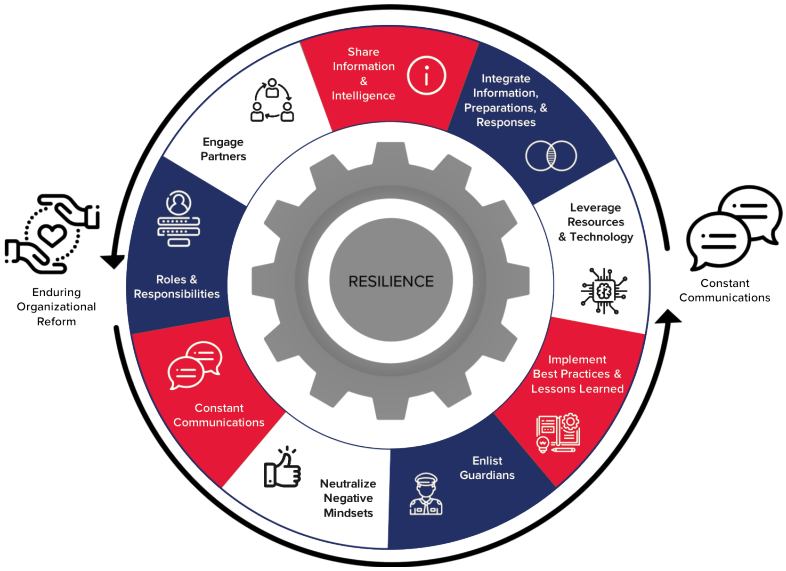
Response – Coordinated Action

Integrated and Coordinated Responses. Prepare and execute those plans before a crisis.
Citizen as First Responder. An elusive predatorial threat forces the average citizen to be thrust forward at an unknown time and place to serve as Citizen First Responder.

Response Times: From First Mitigation to Recovery. What is the response time for law enforcement, fire, and medical?

Take Action!

- ✔ Conduct an Assessment.
- ✔ Draft Plans for Steady State and Crisis.
- ✔ Draft Plans Driven and Guided by the Best Information.
- ✔ Draft an Annual Training and Exercise Schedule
- ✔ Train and Exercise
- ✔ Integrate First Responders into Institutional Planning and Responses.
- ✔ Rehearse the Plan with Stakeholders.
- ✔ Update Plans and Training Based on Gaps Identified During Exercises.
- ✔ Rehearse, Rehearse, Rehearse.
- ✔ Execute Plans in Crisis / Run the Play.



PRINCIPLE 5: LEVERAGE RESOURCES AND TECHNOLOGY

The fifth principle of the RESILIENCE Model is "Leverage Resources and Technology." The key to principle five is to map current resources and seek additional ones through public and private organizations to meet security and communication needs.

An integrated portfolio of public and private resources not only expands the potential resource pool for a house of worship but also provides an additional degree of resilience.

> *Understand the resources you have and the ones you don't, and where you can get them.*
>
> *- Kona Zoganas, House of Worship Director of Security*

✔ **Identify Public Resources -- Federal, State, Local.** The Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI) provide a range of services and tools for houses of worship.

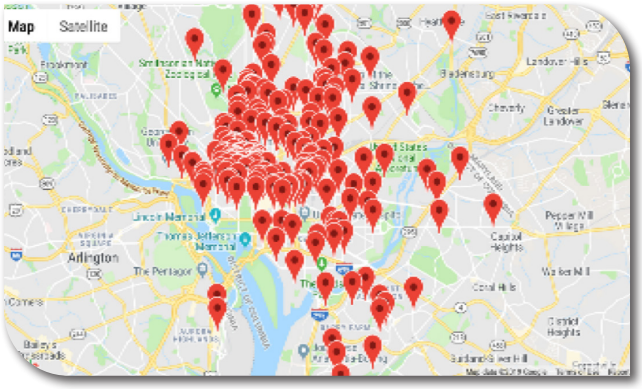
- **Explore** Federal, state and local governments grants for training and security equipment.
- **Research** Federal**,** state and local first responders for training and exercise support.
- **Leverage** security templates, planning checklists from the DHS website and state security websites.

✔ **Identify Private Resources -- Funding (Donors, Sponsors).** Global organizations and national nonprofit organizations can provide financial resources to fund houses of worship security measures and training.

> *Homeland Security, the FBI have great resources that are readily available with pre-built templates that you can tailor and tweak to fit your organization.*
>
> *- Andy Jabbour, Cofounder, FB-ISAO*

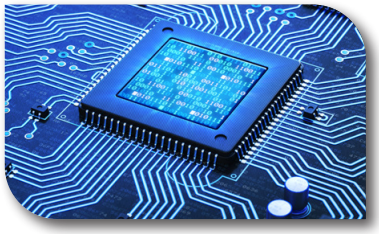
- ✔ **Map Existing Resources:** An inventory captures all of the potential programs and partners in the community and frequently reveals resources and partners not previously identified.

A Community Resource Inventory



- ✔ **Step One Map It.** Map all of the programs and resources in the community that impact, complement, or help your house of worship.
- ✔ **Step Two Be Aware.** Monitor the resources within the immediate and broader community.
- ✔ **Step Three Integrate / Leverage.** Ensure full integration and leverage of all available resources and expertise to fill critical gaps.
- ✔ **Step Four Reduce Duplication.** Duplication might be a sign of inefficiencies in processes or in resources. Reduce unnecessary efforts and to streamline protocols, processes, and procurements.
- ✔ **Step Five Evidence-Based.** Focus on integrating and leveraging evidence-based best practices, technologies, and protocols. Resource and security decisions should be based on evidence.

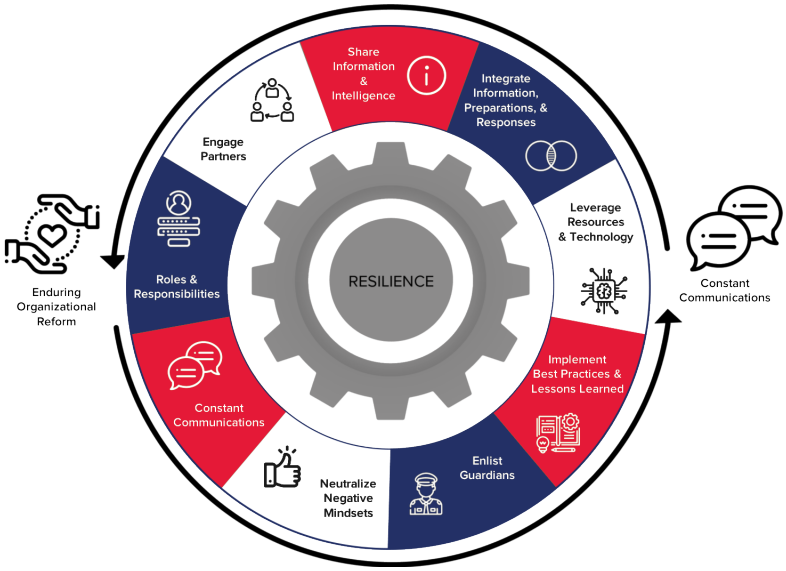
Integrate Technology



- ✔ **Identify and Integrate Technology to Detect "Sense It."**
- ✔ **Cameras to Sense and Inform.**
- ✔ **Identify and Integrate Technology to Deter**
- ✔ **Identify and Integrate Technology to Defend**
- ✔ **Identify and Integrate Technology to Communicate**
- ✔ **Identify and Integrate Technology at the Speed of Life**

Take Action!

- ✔ Assess the Current Resource Picture.
- ✔ Identify All of the Possible Resource Options Internally and Externally.
- ✔ Select the Most Impactful Sources and Actively Pursue these Resources.
- ✔ Start Fundraising and Apply for Grants.
- ✔ **Integrate Technologies to Detect, Deter, And Defend.**



PRINCIPLE 6: IMPLEMENT BEST PRACTICES AND LESSONS LEARNED

The sixth principle of the RESILIENCE Model is "Implement Best Practices and Lessons Learned." Implementing best practices and lessons learned enhances resilience and reduces the threat to vulnerable communities and houses of worship. Remember it is only a lesson learned once implemented.

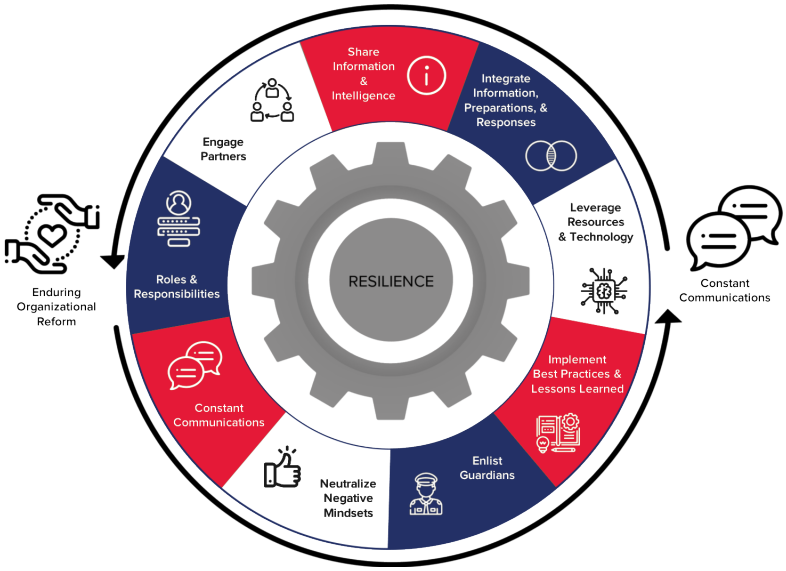
Implement a Lessons Learned Cycle

- ✔ **Key Ideas.** There are three key ideas in this section: one is the establishment of a learning culture, the second is the implementation of lessons learned and best practices, and the third is ensuring that this is a continuous process.
- ✔ **Communicate.** Learning cultures do not just happen. The cultivation of a learning culture requires leaders who drive its development through constant communications, and it requires the active participation of every member.
- ✔ **Implement.** Implement lessons learned, the best practices, or the plan modifications.
- ✔ **Review and Refine.** The next step in the cycle is to review and refine. Reviewing the plan or exercise with stakeholders will help identify and highlight deficiencies and gaps.

Take Action!

- ✔ **Foster a Learning Culture.**
- ✔ Pursue Continuous Learning & Implementation.
- ✔ Learn, Listen, and Implement from Your Experience.
- ✔ Learn, Listen, and Implement from the Experience of Others.
- ✔ Remember—Only a Lesson Learned Once Implemented.
- ✔ **Implement Best Practices Now.**

> *Have a plan, rehearse your plan, and then after you've rehearsed your plan, improve your plan.*
>
> *– Kona Zoganas, House of Worship Director of Security*



PRINCIPLE 7: ENLIST GUARDIANS AND EXECUTE THE PLAN

The seventh principle of the RESILIENCE Model is "Enlist Guardians and Execute the Plan." The focus of this principle is for a house of worship to mobilize guardians and put the plan into execution! Guardians can range from volunteers who serve as ushers welcoming and guiding people into the facility to full-time security staff.

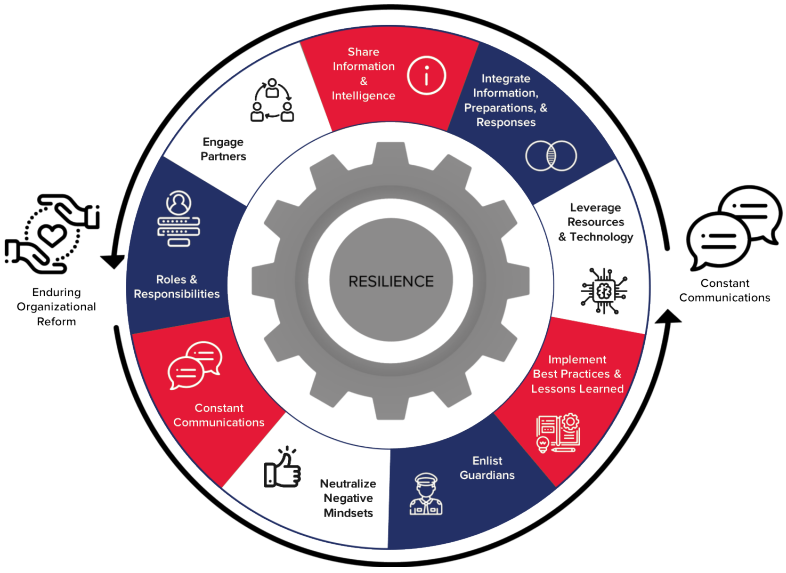
- ✔ **Identify Internal Guardians:** Internal guardians include volunteers and professional staff over whom a house of worship's security leader exercises direct responsibility. Internal guardians are an institution's first line of defense. They are sourced from internal resources and the immediate community.
- ✔ **Identify External Guardians:** External guardians serve as the next layer of complementary security and expertise that further add depth to the safety and security of a house of worship. External guardians include: the local police agency, fire department, emergency medical, and Federal departments and agencies.

> *One of the best lines of defense and your first line of defense are your ushers.*
>
> *- Jeff Ringel, Former FBI*

Execute, Take Action: The absolute key to the security and safety of a house of worship is in the execution of the institution's plans, processes, and protocols. Action is always the key, from engaging partners, to sharing information, to executing the response plan. The current threat environment demands action and the timely execution of plans.

Take Action!

- ✔ Enlist Guardians.
- ✔ Identify and Deploy Internal Guardians.
- ✔ Identify and Deploy External Guardians.
- ✔ **Take Action — Execute, Execute, Execute.**



PRINCIPLE 8: NEUTRALIZE NEGATIVE MINDSETS

> *Terrorism and mass violence cannot prevail if people refuse to be terrorized. If people are resilient, if they return to their houses of worship, the assailant fails...*
>
> *– Jeh Johnson, Former Secretary of the U.S. Department of Homeland Security*

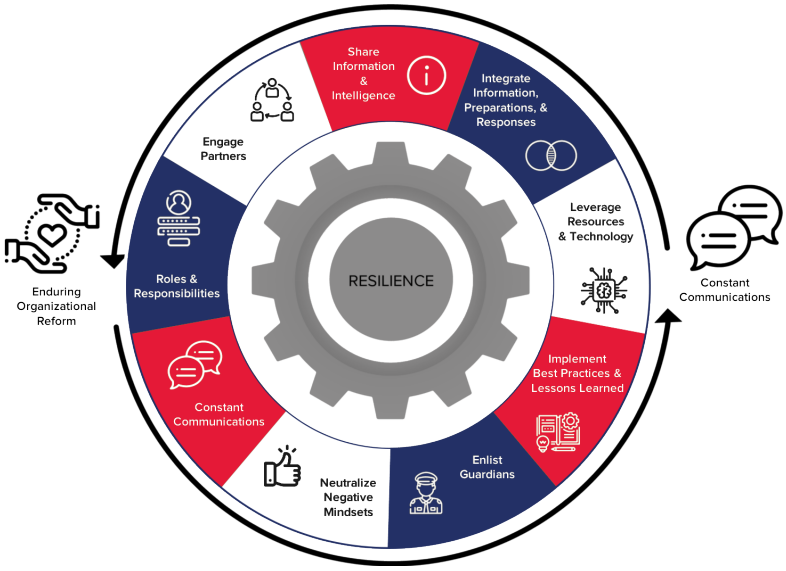
The eighth principle of the RESILIENCE Model is "Neutralize Negative Mindsets." The focus of this principle is to ensure an empowering philosophical and psychological paradigm that rejects negative mindsets. Negative mindsets are driven by false premises such as "this will never happen to us," "what can we do about an active shooter?" or "our faith is enough," or "this is inevitable." Negative mindsets degrade preparations and ultimately, response. They curtail a security culture from taking root. Negative mindsets ignore the dangers to a community and/or disempower individuals.

Mindset and Mental Preparations. Negative mindsets tend to ignore security concerns and underestimate the importance of factoring security considerations into everyday matters. Negative mindsets foster thinking that unfortunate incidents will never happen to one's community or are just inevitable. The right mindset embraces partners and preparations that ensure safety and security.

Take Action!

- ✔ Accurately Assess the Risk.
- ✔ Accept the Reality that Violent Acts can Happen at Any House of Worship.
- ✔ Acknowledge the Possibilities.
- ✔ Talk About It.
- ✔ Ameliorate Fear with Training and Awareness.
- ✔ **Do Not Think "If," Think "When" and "What" to Do.**
- ✔ **Think "We Can and Will Prepare, Prevent, And Mitigate."**

> *Resilience is about mental preparations and how to deal with change.*
>
> *– Bob Liscouski, Former Assistant Secretary, U.S. Department of Homeland Security, Office of Infrastructure Protection*



PRINCIPLE 9: CONSTANT COMMUNICATIONS

The ninth principle of the RESILIENCE Model is "Constant Communications." Houses of worship in constant communication with their partners, guardians, and congregation are better prepared **before, during, and after** an incident.

Link to the World

"Constant Communications" is the pathway that allows for the sounding of the alarm in crisis. It enables the internal and external roles of partners before, during, and after an incident.

"Constant Communication" is vital for coordination and a unified response.

- ✔ Routinize your communications
- ✔ Ensure redundancies in systems and people.
- ✔ Leverage an all source and method approach, from traditional face-to-face meetings to social media.
- ✔ Integrated communication plans with partners.

Internal vs. External Communications

There are two primary communication pathways when working in teams before, during, and after an act of man or nature -- Internal and External Communications.
Internal communications focus within the house of worship. This includes leadership, internal security and safety teams, and the faith community. External communications are focused on partners like first responders, local, state, and Federal departments, the media, and the general public.

Communicate, Communicate, Communicate. The key to building resilience in houses of worship is to talk constantly to all partners and guardians. When communities communicate, they become more prepared, resilient, and ready!

Develop a Communications Plan

Speaking with one voice before, during, and after crisis is essential. The communications plan need not be overly complex. It will address:

- ✔ Who is communicating?
- ✔ What are they communicating? When? Why?
- ✔ The plan must routinize communication channels internally and externally.

The following strategic guidance should be considered:

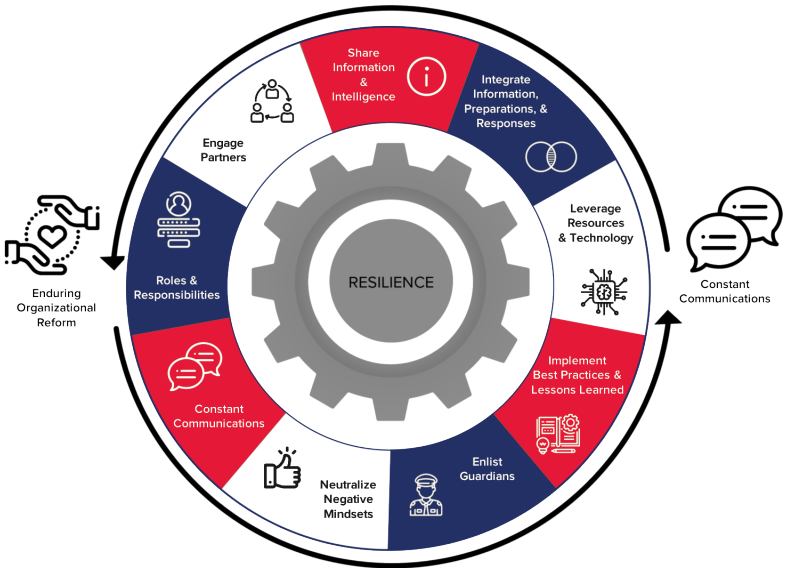
- ✔ Communications will be timely and honest.
- ✔ Staff and the congregation should hear news from the Director of Communications or the head of the congregation first.
- ✔ Provide objective and subjective assessments.
- ✔ Inform all staff at the same time (when possible).
- ✔ Give bad news all at once – do not sugarcoat the truth.
- ✔ Provide the opportunity to ask questions (if possible).
- ✔ Provide regular updates and let people know when the next update will be issued.
- ✔ Communicate in a manner appropriate to circumstances:
  - Face-to-face meetings (individual and group)
  - News conferences
  - Social media
  - Voicemail/email
  - Intranet and internet sites
  - Toll-free hotline
  - Special newsletter
  - Announcements using local/national media
- ✔ **Steady State Communications Plans.** Create a steady state communications plan that allows all stakeholders to communicate on a regular basis.
- ✔ **Crisis Communications Plan**. Think of the creation of the crisis plan as the next layer of communications readiness. The key difference is the context and the need for speed.

Redundancy Equals Reliability and Readiness.

- ✔ Establish the Director of Communications is the primary for the ninth principle.
- ✔ Identify an alternate and tertiary back up for the Communications Director.
- ✔ Train alternate and tertiary directors so they are step up and engage.
- ✔ Building redundancy within the communications personnel, plans, and systems is integral to the safety, security, and resilience of a house of worship.

Take Action!

- ✔ **Communicate Constantly!**
- ✔ Build a Steady State (non-crisis) Plan and Execute.
- ✔ Build a Crisis Plan.
- ✔ All Source Approach (from calls to social media).



PRINCIPLE 10: ENDURING ORGANIZATIONAL REFORMS AND READINESS

The tenth principle of the RESILIENCE Model is "Enduring Organizational Reforms and Readiness." This final principle of the model focuses on the need to codify safety and security practices to ensure lasting reforms and readiness. Reforms must be institutionalized. Readiness must be constant.

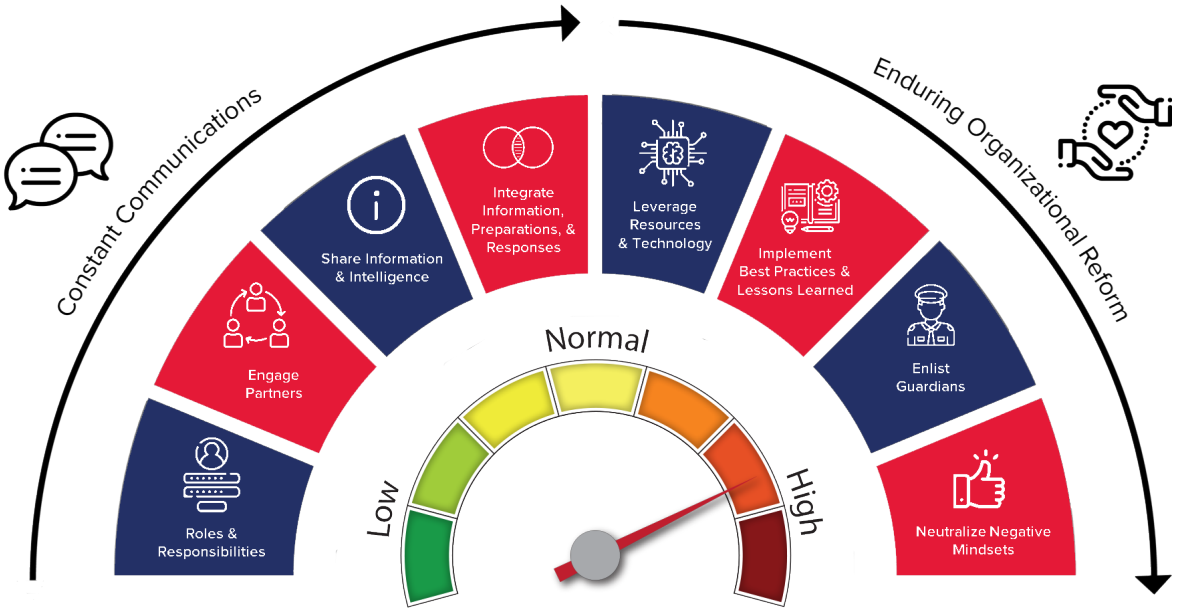
- ✔ **Enduring Reforms—Institution Building.** Houses of worship must institutionalize their success to ensure that lessons learned are documented and implemented. Codify plans, procedures, people, and protocols to lock in the best insights. Security teams must avoid the following perils: no documentation, no dissemination, no follow-up, no institutionalization of reforms.
- ✔ **Enduring Readiness -- Institutional Vigilance.** The current threat picture is increasingly disruptive and unpredictable. Readiness must be a constant priority despite the challenges of strained services and day-to-day challenges. The need to be constantly vigilant and integrate endurance into plans and posture is essential for resilience.
- ✔ **Avoid the Peril of Peek Activity Followed by Protracted Inactivity.** Rare, brief, violent, and chaotic events generate peek activity and hyper-vigilance. The institutional endurance necessary for this level of heightened activity often times does not exist. Hyper-vigilance is frequently quickly followed by dramatic drops in security protocols. Endurance is about pacing. This is not a sprint, but rather a marathon. It is a journey that requires enduring organizational readiness. Avoiding the perils of peek security activity followed by protracted inactivity.

Take Action!

- ✔ Build Enduring Organizational Reforms.
- ✔ Be Ready, Every Day.
- ✔ Create a Sustainable Awareness and Security Posture.

> *You develop resources and institutions that are necessary for creating awareness, creating empowerment, and reassuring the community that their voice can be heard.*
>
> *– Ali Chaudry, NJ Interfaith Advisory Council Member*

RESILIENCE MODEL FOR ASSESSMENT



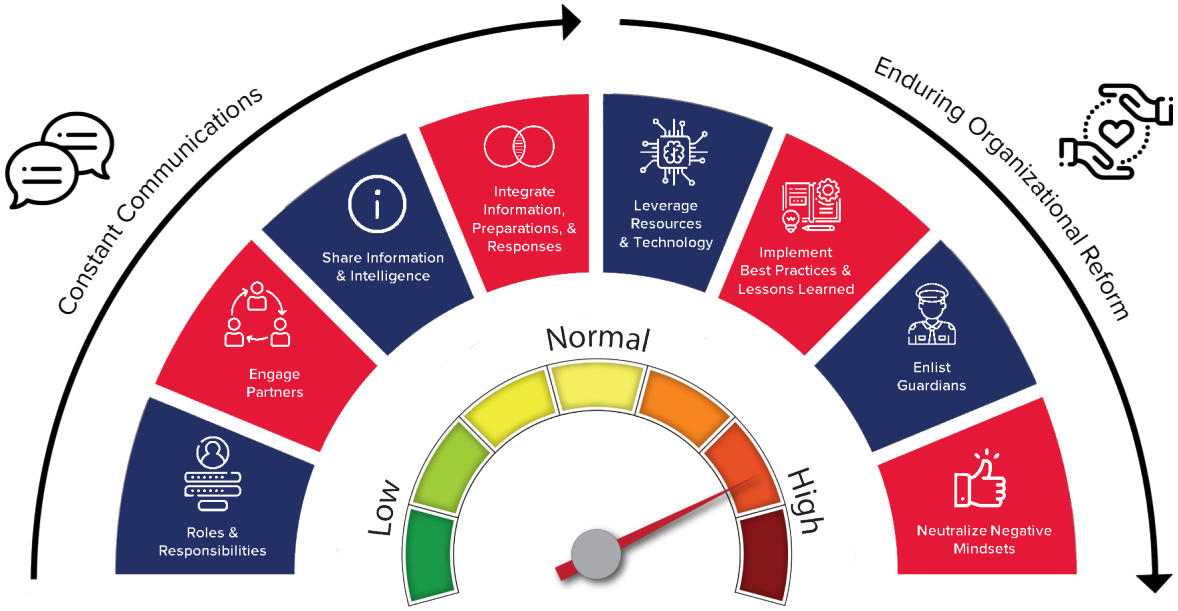
The ten principles of the RESILIENCE Model also serve as an assessment tool. The model serves not only as a system to guide actions and solutions, but when used as an assessment tool, provides a review of institutional or community resilience. Each principle is weighted from 0 to 10 points when used as a rapid assessment, collectively producing a score of 0 to 100. Review of case studies both successful and unsuccessful in mitigating a crisis indicate that scores as low as 70 to 75 can produce sufficient countermeasures to avert disaster. A 70 or a C- might be enough to avert disaster, while case studies with scores in the 30s consistently had tragic consequences.

From Assessment to Action

The RESILIENCE Model provides an assessment that is postured for action. Once assessed along the 10 principles, the assessment phase is naturally mapped to action. This crucial transition from assessing to acting is vital. All too often, institutional assessments of resilience stop at the review process. The RESILIENCE Model is a system designed to reduce friction and enable action. The other key point is that the assessment process is not a static, one-time event. Each assessment is only a snapshot in time, based on current security protocols and threats. As institutions evolve and new threats emerge, security protocols may need to change. Assessing periodically with a set model or methodology also affords the ability to track progress or regression. Thinking of the assessment process as a cycle includes the following options:

- ✔ Annual Assessments
- ✔ Odd / Even Years (Physical / Cyber)
- ✔ Event-Driven Assessments
- ✔ Threat-Driven Assessments
  - General Information and Intelligence Assessments
  - Specific Information and Intelligence Assessments
  - Actionable Intelligence
- ✔ Deliberate and Rapid Assessment Templates

APPENDIX A.1 RAPID RESILIENCE ASSESSMENT



Guidance:

10 Resilience Model Principles each valued at 0 to 10 Points.
Rapid Assessment 10x10 = 100.
Total Valuation from 0 to 100.

Principle	Value	Score
1. Roles & Responsibilities	0 -10	
2. Engage Partners	0 -10	
3. Share Information & Intelligence	0 -10	
4. Integrate Information, Preparations & Responses	0 -10	
5. Leverage Resources & Technology	0 -10	
6. Implement Best Practices & Lessons Learned	0 -10	
7. Enlist Guardians & Execute	0 -10	
8. Neutralize Negative Mindsets	0 -10	
9. Constant Communications	0 -10	
10. Enduring Organizational Reform	0 -10	
Total Score:	0 -100	

APPENDIX A.2 DELIBERATE RESILIENCE ASSESSMENT

Guidance:

10 Resilience Model Principles.
Deliberate Assessment Total Valuation 0 to 100.
Principles 1, 2, 3, 5, 6, 7, 9 valued from 0 to 10.
Principle 4 valued from 0-20 and principles 8 and 10 valued from 0-5.

Principle	Value	Score
1. Roles & Responsibilities Roles Identified (2 points) Responsibilities Identified (2 points) People Identified and Designated (2 points) People Ready to Perform Designated Roles & Responsibilities (4 points)	**0-10** **2** **2** **2** **4**	
Principle 1 Sub Score		
2. Engage Partners Congregation (2 points) Local Community (2 points) Law Enforcement (Local, State, Federal) (2 points) Fire Department and Emergency Medical (2 points) National Organizations, Associations (2 points)	**0-10** **2** **2** **2** **2** **2**	
Principle 2 Sub Score		
3. Share Information & Intelligence (GAS) Gather (4 points) Analyze (2 points) Share... With Congregation and Local Community (2 points) With First Responders and Other Partners (2 points)	**0-10** **4** **2** **2** **2**	
Principle 3 Sub Score		
4. Integrate Information, Preparations & Responses Preparations (Assess: 3 points, Plan: 3 points, Train & Exercise: 4 points) Responses (Before: 4 points, During: 3 points, After: 3 points)	**0-20** **10** **10**	
Principle 4 Sub Score		
5. Leverage Resources & Technology Resources, Public and Private (6 points) Technology (4 points)	**0-10** **6** **4**	
Principle 5 Sub Score		

Principle	Value	Score
6. Implement Best Practices & Lessons Learned Continuous Assessment (5 points) Implementation (5 points)	**0–10** **5** **5**	
Principle 6 Sub Score		
7. Enlist Guardians & Execute Enlist Internal and External Guardians (5 points) Internal: Citizen as First Responder External: First Responders, Funders and Planners Execute, Take Action (5 points)	**0–10** **5** **5**	
Principle 7 Sub Score		
8. Neutralize Negative Mindsets Never Accept the Mindset that an Incident is Inevitable (5 points)	**0–5** **5**	
Principle 8 Sub Score		
9. Constant Communications Steady State (Non-Crisis) Plan and Execution in Place (5 points) Crisis Plan in Place (3 points) All Method and Source Approach (From Calls to Social Media) (2 points)	**0–10** **5** **3** **2**	
Principle 9 Sub Score		
10. Enduring Organizational Reform Institutionalizing Organizations, Actions, and Reforms (5 points)	**0–5** **5**	
Principle 10 Sub Score		
Total Score:	**0–100**	

R.E.S.I.L.I.E.N.C.E. Model Principles

1. Roles and Responsibilities
2. Engage Partners
3. Share Information and Intelligence
4. Integrate Information, Preparations, and Responses
5. Leverage Resources and Technology
6. Implement Best Practices and Lessons Learned
7. Enlist Guardians and Execute the Plan
8. Neutralize Negative Mindsets
9. Constant Communications
10. Enduring Organizational Reform